STRATEGY RESEARCH PROJECT

COMPUTER NETWORK DEFENSE AND ATTACK: INFORMATION WARFARE IN THE DEPARTMENT OF DEFENSE

BY

LIEUTENANT COLONEL CAROLE N. BEST
United States Army

USAWC CLASS OF 2001

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

COMPUTER NETWORK DEFENSE AND ATTACK:
Information Warfare in the Department of Defense

by

LTC Carole N. Best
United States Army

Dr. Robert H. Dorff
Project Advisor

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: LTC Carole N. Best

TITLE: Computer Network Defense and Attack: Information Warfare in the Department of Defense

FORMAT: Strategy Research Project

DATE: 10 April 2001 PAGES: 24 CLASSIFICATION: Unclassified

Our national military strategy paves the way for the Department of Defense (DoD) into the 21st Century. The DoD touts information superiority as being critical to our strategy. However, it has not adequately addressed two key aspects of this "enabler" - the defense of our networks and, should the need arise, attack of those networks belonging to our adversaries.

This paper will discuss current computer network defense and attack policy in the context of ends, ways and means, explain what is lacking in current policy and offer recommendations for improvement. These recommendations include: streamlining the interagency process; exploring a similar structure within the private sector and with our global allies; considering the concept of a separate information corps as a product of increasing emphasis in this area; linking information warfare to other military strategies; and assessing how we will fund the new tools in our information warfare kit bag.

TABLE OF CONTENTS

COMPUTER NETWORK DEFENSE AND ATTACK:
Information Warfare in the Department of Defense

BACKGROUND

Information warfare is the hottest topic in the U.S. military today and with good reason. Because of our post-Cold War advances in technology and the resources to acquire all of the equipment and personnel we need, information warfare (IW) techniques may become the most powerful weapon in our 21st century military arsenal. This emerging heavy reliance on information and technology has dramatically affected how the private sector conducts business and generated a revolution in military affairs within the Department of Defense (DoD). The U.S. military is now exploring how this explosion in technology, along with changes in organization and operations, can improve military effectiveness for the future.

Toward this end, information operations (IO) is now a core consideration in the development of U.S. military policy and strategy, and in the formulation of offensive and defensive operations. Our enemies have come to realize that our intensive reliance on information age technologies is a potential weakness that can be turned into an asymmetric target.[1] The private sector and the DoD recognized this weakness in the mid – 1990's, and the military in particular began to address the issue of information warfare – specifically computer network defense and attack. But although our national military strategy is designed to pave the way for the Department of Defense into the 21st century, DoD has not adequately addressed the two key aspects of our information superiority "enabler" – the defense of our networks and attack of those networks belonging to our adversaries.

This paper will briefly discuss IW in the context of ends, ways, and means from a strategic perspective. This discussion will provide background to our current DoD operational level computer network defense and attack policy, the focus of this effort. It will explain what is lacking in current policy and offer recommendations for improvement. The analysis and recommendations will explore IW failures, both in the current interagency process and in the development of an organizational structure within the private sector and with our global allies. The paper will also address failures at the operational level, specifically the concept of a separate information corps linking information warfare to other military strategies, and in the means to fund the new tools in our information warfare kit bag.

TERMINOLOGY

Before we address the issues surrounding information warfare, and more specifically the defense and attack aspects, we must define the terminology. The Institute for the Advanced Study of Information Warfare defines IW as "the offensive and defensive use of information and information systems to exploit, corrupt or destroy an adversary's information and information systems, while protecting one's own."[2] The problem with this definition is that it is so broad in scope, and so many activities both military and civilian fall under this heading, that it is now difficult to understand exactly what IW is.

James Adams in his book, The Next World War: The Warriors and Weapons of the New Battlefields in Cyberspace, suggests that IW is comprised of three distinct pieces: perception management, where information is the message; destruction, where information is the medium; and information exploitation, where information is an opponent's resource to be targeted. This definition, while not encompassing all of the IO pillars of our joint military doctrine, is closer to the DoD's accepted definition for IW as the "capability to collect, process and disseminate an uninterrupted flow of precise and reliable information, while exploiting or denying an adversary's ability to do the same"[3]. Both of these definitions (the former British, the latter U.S.) are more precise in nature from a military perspective and encompass policymakers, commanders, the forces, the media, the intelligence community and the private sector. From these broader definitions, we can now extract definitions for the computer network defense (CND) and computer network attack (CAN) aspects of IW.

Computer network defense and attack are key components of defensive and offensive Information Operations, respectively. Both are subsets of information warfare, which is further defined by the Army in FM 100-6 as those actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own processes, systems and networks. FM 100-6 further cites CNA as part of Command and Control (C2) Attack, a subset of C2 Warfare. Command and Control Warfare is a subset of IW and Offensive IO. The goal of CNA (used interchangeably in this paper with cyber-attack) is to selectively deny, disrupt, degrade or destroy the enemy's information resident in computers and networks or the computers and networks themselves.[4] Computer network defense attempts to keep the enemy from disrupting or destroying our networks, and is achieved through the use of passwords, encryption devices and sophisticated network monitoring. These emerging components of the IW and IO strategies,

if adequately resourced and implemented, could become the enablers for U.S. military success on the battlefield.

Two serious issues of IW remain unresolved: collateral damage and the rules of engagement. Collateral damage, the unintended consequences of an attack, poses significant challenges for our policy and lawmakers. In a network attack, shutting down an electric transportation system could also terminate all electric power to the hospitals, an unintended target, in the area under attack. How we prevent the unintended from occurring, how we respond in the event it does, and being prepared for the repercussions of the adversary's response to our attack warrant serious consideration. Assessing collateral damage if we are authorized by the National Command Authority (NCA) to attack an adversary's networks is another worrisome issue for the DoD. If we counter the attack by other than covert means, we may legitimize this form of warfare for our adversaries. We are not sure that we are prepared for the repercussions of a counter-attack, as electrons recognize no borders. The rules of engagement, understanding the laws and policies governing an attack, still must be worked out. At present, the NCA retains the right to authorize a cyber-attack, but under what conditions still remains unclear.

Although a computer network attack strategy is not clearly articulated in the most recent U.S. National Security Strategy (NSS), dated December 1999, the NSS does stress the need for the development of capabilities that protect, detect and respond to attacks before they can cause serious damage to our networks and infrastructures. The ability to protect and defend our infrastructures and networks is the strategic "end" that President Clinton's NSS was seeking from the concerted efforts of the DoD, other government agencies and the private sector. The "means" currently available to protect and detect attacks to our networks are through the use of computer authentication, passwords, encryption devices and vigilant monitoring and reporting to other government agencies and the private sector, when these attacks occur. The "ways" that the DoD specifically will protect and defend our infrastructures and networks include: presidential mandates that articulate the roles and responsibilities of federal agencies; assignment of the mission area to an adequately resourced entity willing to establish and implement a CND and CNA strategy; and development of an organizational, reporting, response, recovery and enforcement structure for these evolving mission areas in concert with other federal agencies and the private sector.

NEW THREATS AND CHALLENGES OF INFORMATION WARFARE

The threats and challenges posed by the evolving trends in information technology and warfare are certainly new. We clearly understand conventional warfare; we know the rules and how to play. In information war, we don't know how to play because the rules are not clearly defined for nation-state actors, and non-state adversaries such as terrorist groups, commercial entities or individuals pose an even more difficult challenge. For example, can a nation-state engage in conflict with an individual, or group, and if so what are the rules?

Some theorists cite the Aum Shinri Kyo subway attack in Tokyo as a prime example of what non-state actors can do in "tomorrow's war".[5] This incident involved the use of a biological weapon in the subway system in Tokyo where many people were contaminated and several died. Some may argue the point, but this incident illustrates how IW could provide the means for non-state actors to threaten the security of the Westphalian state. Instead of a biological attack in a subway, this could have been a cyber-attack on an electrical grid of a major metropolitan area, with far more devastating results. A similar, little publicized event in Iraq after the Gulf War resulted in the deaths of 70,000 non-combatants.[6]

Another important aspect of IW defense is how to identify the threat and that we are under attack – both internally (hackers, disgruntled employees) and externally (industrial spies, terrorists groups). According to Former Deputy Secretary of Defense John Hamre, the country is already engaged in a cyber war involving its information infrastructure.[7] These threats are very real and it is virtually impossible to determine with any degree of accuracy how many intrusions into our networks actually occur. Recent studies are alarming. Commercially, seventy–five percent of Fortune 500 companies surveyed in 1998 reported financial losses due to computer security breaches in 1997 alone.[8] Federal Bureau of Investigation (FBI) reports indicate more than 20 foreign governments are systematically vacuuming American multi- national corporations of 24 billion dollars worth of trade secrets and other intellectual assets every year.[9] Another security source indicates that every 20 minutes someone tries to penetrate a DoD computer network.[10] Also, recent GAO reports found that 65% of an estimated 250,000 attacks on DoD systems in 1996 were successful in attaining access. The Department of Defense detected and reported only one out of every 150 unauthorized intrusions.[11] These examples demonstrate just how vulnerable we are to internal and external threats.

Another major threat to our systems is the foreign development of our software. The fact that most of our software is now designed in the Middle East and the Pacific Rim poses a significant potential risk to our infrastructures, critical weapons systems, communications and

economic nodes. It is conceivable that if these developers have interests divergent from ours, they could easily insert destructive code in programs or leave back doors where they could enter our computer systems at will.[12] We must never forget that potential adversaries will have the same technology available to us.

These are but a few of the threats and challenges that we have not begun to address in this new form of warfare. To fail to do so with sound policy, doctrine and adequate resources will undermine our national and military security.

ENDS AND WAYS

The National Security Strategy dated December 1999 states,

> "Our national security and our economic prosperity rest on the foundation of critical infrastructures, including telecommunications, energy, banking and finance, transportation, water systems and emergency services. These infrastructures are vulnerable to computer generated and physical attacks. More than any nation, America is dependent on cyberspace. We know that other governments and terrorist groups are creating sophisticated, well-organized capabilities to launch cyber-attacks against critical American information networks and the infrastructures that depends on them."

This same strategy states that the solutions to protect our infrastructures will come from cooperative efforts between the DoD, other federal agencies, the commercial and private sectors and our allies. However, beyond two Presidential Decision Directives (PDD) 62 (Terrorism) and 63 (Protection of Critical Infrastructures) designed to stimulate the interagency process, there is little evidence that most of these players are aggressively pursuing solutions to the emerging threat.

Currently, the DoD is the most actively engaged in its efforts to develop mechanisms to counter the threat to military systems. The most recent Quadrennial Defense Review (May 1997) addressed IO as a means to shape our environment and respond to new threats. This was translated into our most current National Military Strategy (NMS), and in October 1999, U.S. Space Command (USSPACECOM) was tasked with the mission of "protecting the military's computer networks from cyber-attack."[13] The CND and CNA missions are not new to the military but this is the first time that activities are consolidated and formalized at the joint-service level under a Commander-in-Chief (CINC). In taking this action, U.S. officials signaled their resolve in retaining the overwhelming advantage that U.S. forces presently enjoy over potential adversaries in the multifaceted information operations realm. United States SPACE Command's new operational responsibilities should serve as a warning to prospective

adversaries that a new dimension of warfare is dawning."[14] In formalizing the CND and CNA missions, IO became a "critical interest" of the DoD in attaining information superiority, one of the core enablers of our NMS.

In order to understand the benefits to be gained from a CND and CNA strategy for the DoD, we need to assess them in the context of the NMS. In the most recent version of the NMS, the Chairman, Joint Chiefs of Staff viewed information superiority as the critical "enabler" or "way" to ensure joint forces are dominant across the full spectrum of military operations. These operations include dominant maneuver, precision engagement, focused logistics and full-dimension protection of systems, processes and forces. If information superiority is the way to ensure battle space dominance, we must have effective computer network defense and attack policy, procedures and strategy. The effective implementation of policy, procedures and strategy will help to ensure we attain and retain the ability to develop and execute flexible deterrent options to preclude crises, control the situation in operations other than war and rapidly achieve operational advantage over our adversaries in the event of war.

Presidential Decision Directive 63 (May 1998) on Critical Infrastructure Protection (also a sub-heading under Defending the Homeland in our NSS) provides the strategic level "ways" for how we will defend our networks and infrastructures and respond to attacks on our networks before they cause serious damage. The provisions of this directive seek to achieve our national security and military objectives through the use of interagency coordination for the protection of our critical infrastructures. The PDD articulates the roles and responsibilities of U.S. agencies in fighting terrorism (information warfare falls into this realm) and calls for improvements in capabilities for protecting the national information structure. Establishing partnerships with industry and the private sector to enhance computer security, and developing a plan for minimizing damage and recovering rapidly from attacks to vital infrastructures, are also part of this presidential mandate.[15]

The strategic level guidance in PDD 63 assisted General Ralph Eberhart, CINCSPACE in the development of operational level "ends" for his new CND and CNA missions. In a recent publication, General Eberhart stated that his objectives are to:

> Defend against any unauthorized intrusion into our networks, lead efforts to streamline processes across the DoD, improve global computer network defense and attack capabilities, revise the DoD process for Information Ops Conditions and standardize the way we respond to emerging threats to our networks. [16]

The "ways" the CINC will accomplish his mission are quite similar to those at the strategic level. He must work in partnership with other CINCs, military departments, government

agencies and the private sector to enhance security and minimize damage to DoD networks. Additionally, he must focus on improving our technological and procedural abilities to defend against, respond to and recover from attacks. He will also need to assess and recommend the consolidation and/or elimination of costly duplication of effort within the Services.

THE PROBLEM: INADEQUATE RESOURCES

To successfully execute the CND and CNA missions, resources or means are needed, including trained personnel, hardware and software solutions, funding, and new laws. However, the CINC is lacking in all of these resources. Currently, there are only 39 personnel assigned to the task force responsible for conducting continuous defense operations. "Members of the JTF-CND focus on providing real-time defense to military networks, rather than on developing policy for these activities or working on hardware and software solutions aimed at thwarting unauthorized intrusions into military computer networks."[17] As the CINC officially assumed the CNA mission in October 2000, little more than the establishment of an Activation Task Force designed to study the problem, and to develop and implement plans and concepts of operations for both activities, was in place.

There is little evidence of sufficient funding allocated to support the attack mission. Although it is anticipated that the defense mission will receive almost triple its current $6 million in the FY01 budget, this increase is designated for personnel costs and operating expenses of the JTF-CND. Other issues that have not been adequately addressed are the development of policy, doctrine and new laws governing the CND and CNA missions. It is clearly evident that the resources to implement these missions are grossly out of balance with their criticality. This mis-match in "ways" and "means" poses significant risk to our national military strategy, the underpinning of our national security strategy. Equally alarming is that "presently there is no federally funded organization with responsibility for safeguarding the integrity of computer controlled systems in municipal areas that might be targeted in an effort to impede a military operation, such as a deployment from a U.S. port."[18] Although there is some ongoing interagency coordination to address this problem, those relationships are still evolving.

As stated earlier, information superiority is one of the ways the DoD seeks to achieve success in our national security and military strategies. If we do not provide sufficient resources to protect our systems from intrusion and manipulation we will fall victim to cyber-terrorists who will conceive of unlimited ways to cripple our infrastructures, our power grids, our banking systems, our financial markets, our space-based communications systems and our military.[19]

RECOMMENDATIONS FOR THE FUTURE

We recognize that technological advances have caused a revolution in military affairs within the DoD and acknowledge that these changes will dramatically alter how we will conduct warfare in the future. But there remains much to do in the information operations realm in order to achieve the dominance necessary to ensure our success on the battlefield. We have made a good start at the DoD level by identifying the problem and designating a single focal point (CINCSPACE) for these two missions. The CINC has the responsibility for providing oversight of the myriad of complex tasks and interrelationships involved in this new type of warfare. However, this is only a start. To build on this foundation, we need to do the following at the strategic and operational levels:

PROMOTE THE INTERAGENCY PROCESS

The DoD needs to promote the interagency process and engage the Department of Justice (DoJ), National Security Agency (NSA), and the Federal Bureau of Investigation (FBI), and other government agencies and activities in partnership to assess risks and combat the threat. Presidential Decision Directive 63 has established the framework for this partnering to occur. In this document, the President said that critical infrastructures protection was a national security issue and called for the creation of a national security protection plan to improve our defenses against CNA. He specifically called for a "unique, genuine private-public partnership" because the government cannot unilaterally create a defensive structure for critical infrastructures. The goal of PDD 63 was to establish this structure and organization within three years of its inception to ensure minimal, infrequent disruption to our critical infrastructures.[20]

One of the provisions of PDD 63 mandated promotion of the interagency process as part of the solution to defending our networks. The National Infrastructure Protection Center (NIPC) was created in compliance with this provision. Its creation formalizes the interagency relationship of the DoD, DoJ, NSA, with other federal, state and local agencies on the issues of CNA and CND. But the center currently has the capability only to gather and disseminate information on threats to our infrastructures. It is anticipated that by 2003, the NIPC will become the focal point within the government for threat assessment, warning and response to attacks on our infrastructures. The activities of this center will complement those activities currently conducted by the CINC's JTF – CND/CNA.

ESTABLISH A SIMILAR STRUCTURE WITHIN THE PRIVATE SECTOR

An effective CND and CNA strategy will depend on whether corporate America and industry are willing to partner with the DoD and other federal agencies to protect their infrastructures and networks. Unfortunately, many companies are reluctant to cooperate or coordinate with governmental agencies. Additionally, disagreements over encryption standards, antitrust laws and other issues have strained the relationship between government agencies, the DoD and the private sector. The military has little influence over what industry does as consumers are now the more important customers. This makes planning for IW terribly complex. The government, and particularly the DoD, will need to improve relations with companies in the information industry, which need to understand their own stake in an effective defense.[21]

The NIPC, when adequately resourced and fully functional, will provide the needed link between government and industry for the CNA and CND missions. Former Deputy Secretary of Defense John Hamre recently described the activities and functions of NIPC in this way:

> "at the NIPC, we are taking steps to design and implement a national indications and warning system to detect, assess, and warn of attacks on critical private sector and government systems. This involves gathering information from all available sources, analyzing it, and sharing it with all affected entities, public or private. We are also designing a plan to coordinate the activities of all agencies and private sector entities that will be involved in responding to an attack on our infrastructures. These efforts to improve our ability to prevent and respond are critical if we are to be prepared to face the most serious challenges of the Information Age".[22]

Given some estimates that as much as 90 percent of the country's eight critical infrastructures (telecommunications, banking and finance, water supply systems, transportation, emergency services, government operations, electrical power, and gas and oil storage and delivery) are privately owned, this partnership between government and industry is crucial to protecting and defending our national infrastructures. The NIPC (via the Information Sharing and Analysis Centers) will link government with industry by providing nation-wide information sharing about threats and vulnerabilities, conducting computer security monitoring and network analysis, and assisting with criminal prosecution of attackers.

DEVELOP POLICIES, PROCEDURES AND LAWS WITH GLOBAL ALLIES

A global economy, complex international organizations, a growing worldwide information grid, and countless other interlocking systems now support modern civilization.[23] Based on extensive study of the future global information environment, the leadership of this country believes that the risk of a serious disruption of our national security and economy by hostile

sources will grow in the absence of concerted national action.[24] Our DoD and intelligence communities are watching the IW capabilities of 120 potential adversaries with growing concern. These adversaries either have or are developing the technical capabilities needed for offensive computer operations, and the targets are our civilian information infrastructures, and our military forces.

As we are assessing the capabilities of our potential adversaries, they are likewise watching us. They are aware that we are likely to anticipate, deter, and respond if attacked. By reducing the vulnerability of our critical infrastructures, we raise the bar for those who might consider an attack and reduce the national consequences if one occurs. Presidential Decision Directive 63 provides national strategic direction for redressing the vulnerabilities in our information and other critical infrastructures.[25] Because as an attack on many of our institutions will likely have a ripple effect beyond our shores, the national plan, as it is developed by NIPC, must address how we will interface with our allies. It must also establish for the DoD, as the lead agency for national security, the parameters for and legal ramifications of a counter-attack against a foreign-based attacker.

CONSIDER THE CONCEPT OF A SEPARATE INFORMATION CORPS

As a result of increasing emphasis in this area, Deputy Secretary of Defense Rudy de Leon recently approved a plan that will establish the first ever Joint Reserve Virtual Information Operations /Information Assurance Organization (JRVIO) from National Guard and Reserve units. Recruitment of the initial 182-member force will begin in FY01 with the total strength expected to reach 600 for the five reserve units by FY07. Each JRVIO will directly support the DoD's key information operations agencies and joint commands: the Defense Information Systems Agency; JTF-CND belonging to CINCSPACE; NSA and the Information Operations Technical Center; and the Joint Information Operations Center. Although the goal of this initiative is to better integrate the Guard and Reserve into the Total Force, the outcome, once implemented, will specifically address one of the CINC's shortfalls of trained personnel previously addressed in this paper. Although not specifically stated, it is anticipated that these new units will assist in establishing IW doctrine, developing battle plans and carrying them out, promoting jointness where it is critically needed, elevating information as an element of war, developing an information warrior ethos, and heightening DoD attention to the global civilian net.[26]

FUNDING REQUIREMENTS

The goals discussed in this paper are ambitious and expensive. Democracies generally do not like to spend money on defense in peacetime, for the excellent reason that such expenditures detract from other areas of higher political, social, and economic importance. In a period in which we have no "peer competitors" on the horizon, it will be all the more difficult to convince Congress to allocate resources, including technology, to defense.[27] The DoD plans to spend roughly four billion dollars between 1999 - 2002 on the security of our networks and infrastructures. One NSA source estimates that more than 18 billion dollars will be needed over the next ten years to close the information system security gap.[28] Clearly, given the risks we face today, what we intend to spend on the protection of our networks and infrastructures is inadequate.

Further exacerbating the funding problem is the way our current budget process works. Department of Defense funding is programmed and allocated on a five-year cycle. Information technology changes every six months and the government takes five years to respond to it. With the way we fund our programs, how many generations of technology will develop before we figure out how to respond to the first generation? Can we afford the risks associated with business as usual? This author thinks not. What we need to do in terms of technology is to adopt the rapid acquisition practices of the private sector and adapt them to the military procurement process. We have begun these efforts in earnest with the transformation of the Army and should continue to expand the scope of these processes in support of IO and IW.

CONCLUSION

In the history of warfare, it seems clear that new technologies have resulted in radical reorganizations of the armed forces and transformed the practice of war. Those who adapt have conquered, while those who remain stagnant have been vanquished.[29] This paper concludes that we are already under cyber-attack and might well be on the verge of being vanquished if we fail to properly resource a strategy for the protection of our critical networks and infrastructures. Our current strategy is predominantly defensive in nature and is insufficient to meet the growing threats and challenges to our systems. We have failed to adequately resource both the attack and defense missions, and little beyond the efforts of the DoD are being implemented to protect our networks and critical infrastructures.

Technology is the way of the future for the 21st century. Computers are at the core of every aspect of our existence, from controlling critical infrastructures to conducting military operations. Clearly, computer network defense and computer network attack are in their infancy

and much remains to be done in both arenas. However, we will never successfully protect our infrastructures or attain information superiority on the battlefield until our ends, ways and means are in balance for our computer network attack and defense missions. The current mis-match in "ways" and "means" poses significant risk to our national security and military strategies. Our inability to quickly achieve this balance will lead to potentially catastrophic failure in the face of an attack and pave the way for our adversaries to make these techniques the most powerful weapons in their 21st Century arsenal.

WORD COUNT = 4659

ENDNOTES

[1] Robert H. Scales, "Adaptive Enemies–Achieving Victory by Avoiding Defeat," Joint Force Quarterly, (Autumn/Winter 1999–2000): 13.

[2] Vernon J. Ehlers, "Information Warfare and International Security," The Officer (September 1999): 28.

[3] John M. Shalikashvili, National Military Strategy of the United States of America–Shape, Respond, Prepare Now: A Military Strategy for a New Era, (Washington, D.C.: September 1997), 18.

[4]U. S. Department of the Army, Information Operations. U. S. Army Field Manual 100-6 (Washington, D.C.: Department of the Army, 27 August 1996) 2-3 and 2-4; and Ibid GL- 4-7. The terms are defined as follows:

CNA are operations to disrupt, deny, degrade or destroy information resident in computers and computer networks, or the computers and networks themselves.

C2 Attack is the synchronized execution of actions taken to accomplish established objectives that prevent effective C2 of adversarial forces by denying information to, by influencing, by degrading, or by destroying the adversary C2 system.

C2 Warfare is the integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary C2 capabilities, while protecting friendly C2 capabilities against such actions.

Information Warfare are actions taken to achieve information superiority by affecting adversary information, information based processes, information systems and computer-based networks while defending one's own information, information based processes, information systems and computer-based networks

Information Operations are continuous military operations within the Military Information Environment that enable, enhance and protect the friendly forces ability to collect, process, and act on information to achieve an advantage across the full range of military operations: IO include interacting with the global information environment and exploiting or denying an adversary's information and decision capabilities.

Information Dominance is the degree of information superiority that allows the possessor to use information systems and capabilities to achieve an operational advantage in a conflict or to control the situation in operations other than war while denying those capabilities to the adversary.

[5]Brent Stuart Goodwin, "Don't Techno For An Answer: The False Promise of Information Warfare," Naval War College Review, (Spring 2000): 216.

[6]Byard Q. Clemmons and Gary D. Brown, "Cyber Warfare: Ways, Warriors and Weapons of Mass Destruction," Military Review, (September/October 1999): 44.

[7]William Jackson, "DOD Set to Fight Hackers Both Foreign and Domestic," Government Computer News, Vol. 18, no. 27 (23 August 1999): 8.

[8] Lou Anne DeMattei, "U.S. Vulnerability to Cyber Threat." Officer Review, 39 (October 1999): 22.

[9]Tabassum Zakaria, "Economic Espionage Seen As Growing Threat to U.S. Firms," available from http://cnn.com/2000/TECH/computing/02/15/hacking.investigation.02/index.html, Internet, February 2000, accessed November 2000.

[10]Katherine M. Peters, "Information Insecurity," Government Executive, (April 1999): 18.

[11]DeMattei, 22.

[12]Byard Q. Clemmons and Gary D. Brown, "Cyber warfare: Ways, Warriors and Weapons of Mass Destruction," Military Review, (September/October 1999): 44.

[13]John G. Roos, "Cyber-Sleuths & Cyber-Saboteurs–USSPACECOM Readies for Computer Network Attack Mission," Armed Forces Journal, (September 2000): 38.

[14] Ibid.

[15]Michael Vatis, "National Infrastructure Protection Center Homepage." Available at http://www.nipc.gov/about/about3.htm. Accessed 10 December 2000.

[16]Roos, 43.

[17]Ibid., 40.

[18] Ibid.

[19]William S. Cohen, Defense News, (11-17 May 1998); quoted in Byard Q. Clemmons and Gary D. Brown, "Cyber warfare: Ways, Warriors and Weapons of Mass Destruction," Military Review, (September/October 1999): 43.

[20]Richard Clarke, National Coordinator for Security, Infrastructure Protection, and Counter-terrorism, White House Press Briefing, 22 May 1998 http://www.fas.org/irp/news/1998/05/980522-wh.3htm accessed 15 November 2000.

[21]Bruce D. Berkowitz, "War Logs On: Girding America for Computer Combat", Foreign Affairs, Vol. 79, no. 3 (May/June 2000): 10.

[22]John J. Hamre, Michael A. Vatis, and Arthur K. Cebrowski, "Infrastructure Vulnerability," Issues in Science and Technology, Vol. 15, no. 2 (Winter 1998-1999): 12.

[23]Ibid., 15.

[24]Ibid.

[25]Edward Waltz, "U.S. Transition to Information Warfare," Journal of Electronic Defense (December 1998): 38.

[26]"Reserve Component Units for Information Warfare," Army, (January 2001): 57.

[27]"High Tech: The Future Face of War? A Debate," Commentary, Vol. 105 (Jan. 1998): 33.

[28] Lou Anne DeMattei, "Developing A Strategic Warning Capability for Information Defense," Defense Intelligence Journal Vol. 7 no. 2 (Fall 1998): 89.

[29] High Tech: The Future Face of War? A Debate," Commentary, Vol. 105 (Jan. 1998): 30.

BIBLIOGRAPHY

Bayles, William J. Moral and Ethical Considerations for Computer Network Attack as a Means of National Power in the Time of War. Strategy Research Project. Carlisle Barrack: U.S. Army War College, 24 May 2000.

Busby, Daniel J. Peacetime Use of Computer Network Attack. Strategy Research Project. Carlisle Barrack: U.S. Army War College, 20 June 2000.

Berkowitz, Bruce D. "War Logs On: Girding America for Computer Combat." Foreign Affairs. Vol. 79, No. 3 (May/June 2000): 8-12.

Clarke, Richard. National Coordinator for Security, Infrastructure Protection and Counter-terrorism. White House Press Briefing, 22 May 1998 http://www.fas.org/irp/news/1998/05/980522-wh.3htm. Accessed 15 February 2001.

Clemmons, Byard Q. and Gary D. Brown, "Cyber Warfare: Ways, Warriors and Weapons of Mass Destruction." Military Review. (September/October 1999): 35-46.

Clinton, William J. A National Security Strategy for a New Century. Washington, D.C.: The White House, October 1999.

Cohen, William S. Defense News. (11-17 May 1998); quoted in Byard Q. Clemmons and Gary D. Brown, "Cyber Warfare: Ways, Warriors and Weapons of Mass Destruction," Military Review. (September/October 1999): 43.

DeMattei, Lou Anne. "Developing A Strategic Warning Capability for Information Defense." Defense Intelligence Journal, Vol. 7 No. 2 (Fall 1998): 89.

_____ "U.S. Vulnerability to Cyber Threat." Officer Review. Vol. 39 (October 1999): 22-24.

Ehlers, Vernon J. "Information Warfare and International Security." The Officer. (September 1999): 28-32.

Goodwin, Brent Stuart. "Don't Techno For An Answer: The False Promise of Information Warfare." Naval War College Review. (Spring 2000): 215-224.

Hamre, John J., Michael A. Vatis, and Arthur K. Cebrowski, "Infrastructure Vulnerability." Issues in Science and Technology. Vol. 15, No. 2 (Winter 1998-1999): 10-15.

"High Tech: The Future Face of War? A Debate," Commentary. Vol. 105 (Jan. 1998): 28-34.

Jackson, William. "DOD Set to Fight Hackers Both Foreign and Domestic." Government Computer News. Vol. 18, No. 27 (23 August 1999): 8.

Peters, Katherine M. "Information Insecurity." Government Executive. (April 1999): 18.

President's Commission on Critical Infrastructure Protection. Critical Foundations: Protecting America's Infrastructures. Washington, D.C.: U.S. Government Printing Office, 13 October 1997.

"Reserve Component Units for Information Warfare." Army. (January 2001): 57.

Roos, John G. "Cyber-Sleuths & Cyber-Saboteurs–USSPACECOM Readies for Computer Network Attack Mission." Armed Forces Journal. (September 2000): 38.

Scales, Robert H. "Adaptive Enemies–Achieving Victory by Avoiding Defeat." Joint Force Quarterly. (Autumn/Winter 1999–2000): 13.

Shalikashvili, John M. National Military Strategy of the United States of America–Shape, Respond, Prepare Now: A Military Strategy for a New Era. Washington, D.C., September 1997.

U. S. Department of the Army. Information Operations. U.S. Army Field Manual 100 - 6. Washington, D.C.: U.S. Department of the Army, 27 August 1996.

Vatis, Michael. "National Infrastructure Protection Center Homepage." Available at http://www.nipc.gov/about/about3.htm. Accessed 10 February 2001.

Waltz, Edward. "U.S. transition to Information Warfare." Journal of Electronic Defense. (December 1998): 38

Zakaria, Tabassum. "Economic Espionage Seen As Growing Threat to U.S. Firms." Available at http://cnn.com/2000/TECH/computing/02/15/hacking.investigation.02 /index. html, Internet. Accessed 10 November 2000.